DUE DATE: DEC. 1, 2005

1. Suppose we're working in $\mathbb{F}_2$, and we start with the vectors

$$\vec{v}_1 = (0,1,1,1,1,0),\ \vec{v}_2 = (1,1,1,0,1,0),\ \text{and}\ \vec{v}_3 = (1,0,1,0,0,1).$$

Our idea is that we'll encode three digits (c_1, c_2, c_3) by sending the linear combination $c_1\vec{v}_1 + c_2\vec{v}_2 + c_3\vec{v}_3$ instead.

(a) Let W be the subspace of $\mathbb{F}_2^6$ spanned by $\vec{v}_1$, $\vec{v}_2$, and $\vec{v}_3$. Show that W is three dimensional.

(b) Find *three* equations (it will take at least three) of the form $a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + a_5x_5 + a_6x_6 = 0$ so that W is exactly the solution to those three linear equations.

(c) Find a linear transformation $T : \mathbb{F}_2^6 \longrightarrow \mathbb{F}_2^3$ so that W is exactly the kernel of T.

(d) Can our coding system detect and correct a single error? Explain why or why not.

2. Suppose we're working with numbers in $\mathbb{F}_3$, and we start with the vectors

$$\vec{v}_1 = (1,2,0,1),\ \text{and}\ \vec{v}_2 = (2,2,1,0).$$

We will encode a message (c_1, c_2) of two digits (but now in $\mathbb{F}_3$) by sending the linear combination $c_1\vec{v}_1 + c_2\vec{v}_2$.

Suppose we receive the vector $\vec{v} = (2,0,2,2)$.

(a) Let W be the subspace of $\mathbb{F}_3^4$ spanned by $\vec{v}_1$ and $\vec{v}_2$. Find a linear transformation $T : \mathbb{F}_3^4 \longrightarrow \mathbb{F}_3^2$ so that W is the kernel of T.

(b) Can our code detect and correct a single error? Explain why or why not.

(c) Show that $\vec{v}$ is not in W. Assuming that $\vec{v}$ is only wrong in a single digit, find that digit, correct it, and decode the vector as (c_1, c_2). Explain your steps.

(d) Suppose that we receive $\vec{v} = (2,1,1,1)$. Again assuming that there is only an error in a single digit, correct it and decode the message.

(e) Suppose we receive $\vec{v} = (1,0,1,0)$. If it is only wrong in a single digit, what digit must that be?

(f) Suppose the vector $\vec{v}$ from part (e) were wrong in two digits. How many different possibilities of two digit errors are there? (Two digits means that two digits really change, not that two digits and fewer change). Assuming that there was an error of two digits, list all the possible corrected vectors (the vectors after we fix the errors).

3. The following problem is not a problem in linear algebra, but just a problem in computing with the numbers in $\mathbb{F}_p$, and in understanding a bit about how polynomials factor.

(a) Suppose we look at polynomials of the form $x^2 + ax + b$ with a and b in $\mathbb{F}_3$, and ask whether or not it has any roots. Some polynomials do, for instance $x^2 + 2$ has $x = 2$ as a root, and some don't, for instance neither $x = 0$, $x = 1$, or $x = 2$ are a root of $x^2 + 1$ in $\mathbb{F}_3$.

There are a total of three degree 2 polynomials of the form $x^2 + ax + b$ in $\mathbb{F}_3$ with no roots. One of them is the polynomial $x^2 + 1$ above. Find the other two.

(b) If we compute in $\mathbb{F}_2$, there is only one polynomial of degree 2 which has no roots (it's $x^2 + x + 1$). There are however two polynomials of degree three (of the form $x^3 + ax^2 + bx + c$, with a, b, c in $\mathbb{F}_2$) with no roots. Find both of them.

(c) If we look at degree four polynomials $x^4 + ax^3 + bx^2 + cx + d$ (with all coefficients in $\mathbb{F}_2$) there are actually four which don't have any roots. Find all four.

(d) A polynomial is called *reducible* if it can be factored as the product of lower degree polynomials, and *irreducible* if it cannot. If a polynomial has a root, it must be reducible, since if $x = a$ is a root, then $(x - a)$ must be a factor.

For instance, the polynomial $x^2 + 2$ (working in $\mathbb{F}_3$) factors as $(x + 1)(x + 2)$, so it is reducible. The polynomial $x^3 + 1$ factors as $(x^2 + x + 1)(x + 1)$ (working in $\mathbb{F}_2$) so it is reducible too. The polynomial $x^2 + x + 1$ turns out not to factor at all (working in $\mathbb{F}_2$ again) so it is irreducible.

If a degree four polynomial factors, it must factor as either a degree three polynomial times a degree one polynomial (in which case it has a root), or as the product of two degree two polynomials.

There are only three irreducible degree four polynomials if you work in $\mathbb{F}_2$, find all three.